# Hybrid Encryption Algorithm Integrating AES-256 and RNA Schemes for Enhanced Secure

MEENA DEVI R

*Assistant Professor(SG) Department of Electrical and Electronics Engineering,*

*KCG College of Technology Chennai, Tamil Nadu, India.*

*Abstract:* - The objective of this research is to design and implement a robust encryption algorithm with enhanced security features. Advanced Encryption Standard (AES-256): Due to its efficiency and security, AES-256 is a popular symmetric encryption technique. It is very hard to crack since it encrypts and decrypts data using a 256-bit key. RNA (Ribonucleic Acid) Scheme: This might be an encryption technique that is modelled after the principles of RNA molecules and is physiologically inspired. In this case, it could refer to a cryptographic technique that improves encryption by drawing on ideas from biology or RNA. Combinatorial Method: When combining AES-256 with RNA, one possible method is to use AES-256 for symmetric data encryption.

*Key-Words:* - AES, RNA, hybrid encryption, Data Integrity, security

## 1. Introduction

In order to provide safe communication via unreliable channels, hybrid encryption methods are essential [1],[2]. In order to improve data transmission security, this research suggests a unique method that combines RNA methods with the reliable AES-256 algorithm. Symmetric encryption powerhouse AES-256 is highly renowned for providing a great degree of security. RNA systems, on the other hand, provide an extra degree of protection and complexity, making it even harder for unauthorised parties can intercept and decrypt the data [3],[4],[5].

Our approach seeks to provide a more effective and safe way to encrypt data by merging these two methods. By combining the benefits of RNA with AES-256[7], this method provides improved defence against a range of online dangers, such as data manipulation and eavesdropping. Furthermore, the incorporation of RNA schemes presents novel approaches to key management, which bolster the communication process' security even more [8],[9].

In this paper, we present a thorough explanation of our hybrid encryption method, emphasising its essential elements and the ways in which it guarantees secure communication [10],[11]. We further show our approach's superiority in terms of efficiency and security by comparing it with other encryption algorithms already in use. Our goal is to improve the security of communication networks across multiple domains and progress encryption technologies through this research [12],[13].

This work aims to improve secure communication through the development, testing, and assessment of a hybrid encryption algorithm that combines the AES-256 and RNA methods. The following major points will be the emphasis of the paper:
Algorithm Design: a thorough explanation of the hybrid encryption algorithm that combines the RNA and AES-256 techniques for increased security [14].
Key Management: The method makes use of cutting-edge key management strategies to protect encryption keys and guarantee their appropriate distribution among parties involved in communication.
Data Integrity: Techniques for preserving data integrity and guarding against illegal changes made while it's being transmitted.
Security Analysis: a thorough evaluation of the

suggested algorithm's security advantages and disadvantages, including any potential weak points and defences.
Comparison with Existing Methods: To show how much better the suggested strategy is, a comparison with other encryption techniques and hybrid encryption algorithms that are currently in use.
Practical Applications: A discussion of how the suggested algorithm might be used in real-world situations, with an emphasis on how it might improve secure communication.
Future Research Directions: Building on the conclusions and understandings from this study, recommendations for future paths in the field of hybrid encryption and secure communication.
The purpose of this work is to present a thorough knowledge of the suggested hybrid encryption algorithm and how it might improve safe communication across a range of areas by addressing these concerns[15].

## 2. EXISTING SYSTEM

Several encryption techniques are utilised in the current system to secure communication however their efficiency and security are frequently compromised. A popular method for symmetric encryption is to utilise AES-256 because of its effectiveness and security. Key distribution and administration, however, can be difficult, particularly in large-scale systems or across unreliable channels.

The suggested hybrid encryption technique combines RNA algorithms with AES-256 to overcome these issues. Symmetric encryption, which offers a high degree of security for data transfer, uses the AES-256 algorithm. The integration of RNA methods improves key distribution and administration while bolstering encryption security with an extra layer.

The RNA schemes could improve encryption key creation and administration by utilising ideas from biological RNA molecules, such as genetic or evolutionary algorithms. These programmes can offer a safer and more effective method of managing encryption keys, enhancing the communication system's overall security.

In general, the goal of integrating RNA and AES-256 methods into the current system is to overcome the drawbacks of conventional encryption algorithms and offer a more effective and safer alternative for secure communication.

## 3. PROPOSED SYSTEM

It Several important areas of research and development are involved in the related work in the realm of hybrid encryption algorithms incorporating AES-256 and RNA methods for increased secure communication. The proposed system flow diagram shown in Fig1.

AES-256: Because of its powerful security features and effectiveness, AES-256 is frequently used as a core encryption algorithm in research. These studies frequently investigate various operating modes and optimisation strategies to enhance security and performance.

RNA Schemes: Although less prevalent, research on RNA schemes in encryption is becoming more and more interesting. A few research investigate the use of RNA-inspired algorithms—like genetic algorithms—for encryption systems' key creation and management. These methods seek to improve encryption security and efficiency by utilising RNA principles.

Hybrid Encryption: A number of research studies have been conducted on hybrid encryption strategies that include both symmetric and asymmetric encryption techniques. These studies frequently concentrate on harnessing the advantages of both types of encryption to improve overall security, as well as key distribution and administration.

Secure Communication: Research on key management systems, encryption protocols, and secure data transmission techniques are all included in this category. The goal of these efforts is to create more reliable and effective methods for safe communication across unreliable channels.

Comparative Analysis: A few studies compare various encryption techniques, methods, and algorithms, including hybrid encryption schemes. These assessments determine which encryption technology is best suited for a certain application by weighing its security, effectiveness, and usability.

The suggested hybrid encryption algorithm seeks to improve secure communication systems by offering a more practical, secure, and effective method for data encryption and transmission by expanding on the body of work already done in these domains.

To improve safe communication, the suggested method combines the distinctive qualities of RNA systems with the powerful encryption of AES-256. The system seeks to offer a high degree of protection against a variety of cryptographic assaults by fusing the power of AES-256 with the adaptability of RNA methods. While RNA methods add extra levels of complexity and unpredictability, increasing their resistance to decryption attempts, AES-256 guarantees robust symmetric encryption. By combining the best features of both encryption techniques, this hybrid strategy ensures the security and integrity of sensitive data while constructing a more reliable and resilient communication system.

## 4. METHODOLOGY

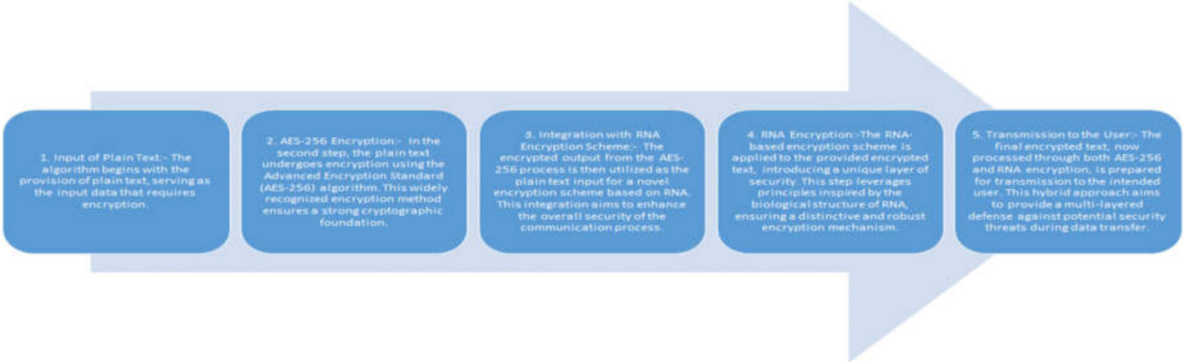

1. Input of Plain Text:- The algorithm begins with the provision of plain text, serving as the input data that requires encryption.
2. AES-256 Encryption:- In the second step, the plain text undergoes encryption using the Advanced Encryption Standard (AES-256) algorithm. This widely recognized encryption method ensures a strong cryptographic foundation.
3. Integration with RNA Encryption Scheme:- The encrypted output from the AES-256 process is then utilized as the plain text input for a novel encryption scheme based on RNA. This integration aims to enhance the overall security of the communication process.
4. RNA Encryption:-The RNA-based encryption scheme is applied to the provided encrypted text, introducing a unique layer of security. This step leverages principles inspired by the biological structure of RNA, ensuring a distinctive and robust encryption mechanism.
5. Transmission to the User:- The final encrypted text, now processed through both AES-256 and RNA encryption, is prepared for transmission to the intended user. This hybrid approach aims to provide a multi-layered defense against potential security threats during data transfer.

Fig1: proposed system flow diagram

There are numerous crucial elements in the process of creating the hybrid encryption algorithm that combines the AES-256 and RNA methods for more secure communication. The structure of the method is first described, including the key generation, encryption, and decryption procedures as well as the integration of the AES-256 and RNA schemes. Subsequently, the implementation of AES-256 encryption and decryption methods guarantees compliance with the selected programming language and platform. For key generation and management, RNA-inspired algorithms—like genetic algorithms—are then chosen and put into practice. Along with methods for guaranteeing data integrity and authenticity, key management strategies that make use of RNA schemes for secure key exchange and distribution are created and put into practice. The performance of the algorithm is assessed in terms of speed, resource consumption, and scalability, and a comprehensive security analysis is carried out to find and fix any potential flaws. Ultimately, the algorithm undergoes multiple scenarios of testing to verify its security and effectiveness, and a documentation outlining the algorithm's concept, implementation, and test outcomes is created. After being presented at conferences or workshops, the algorithm and its results are subsequently published in scholarly journals or other pertinent publications for peer review and distribution.

## 5. IMPLEMENTATION

In this proposed system, taken the following actions to put into practice the hybrid encryption method that combines the AES-256 and RNA techniques for more secure communication:

Algorithm Design: Describe the key generation, encryption, and decryption procedures as well as the structure of the algorithm, including the integration of the AES-256 and RNA methods. It’s shown in Fig2.

AES-256 Implementation: To implement AES-256 encryption and decryption capabilities, use a cryptographic library. Verify that it works with the programming language of your choice.

RNA Scheme Implementation: Use RNA-inspired key generation and management techniques, including genetic algorithms. Verify if they work with the programming language you use.

Key Management: Create key management strategies that make use of RNA schemes to distribute and exchange keys in a secure manner. Put in place procedures for safely storing and obtaining encryption keys. It’s shown in Fig3.

Data Integrity: Fig4 shows the provide systems, like digital signatures or checksums, to guarantee the authenticity and integrity of data. Incorporate these techniques into the procedures of encryption and decryption. Security study: To find and fix possible vulnerabilities, perform a comprehensive security study. If necessary, apply more encryption layers or security measures to the algorithm to increase its security.

Performance Evaluation: Assess the scalability, resource consumption, and encryption/decryption speed of the algorithm. Compare it to the current encryption techniques.

Testing: To ensure the algorithm's security and effectiveness, test it in various contexts. Make sure it functions as planned in a variety of scenarios.

Documentation: Keep a record of the test findings, implementation specifics, and algorithm design. Give precise directions on how to apply the algorithm in real-world scenarios.

Presentation and Publication: Give a conference or workshop presentation of the algorithm, methods, and results. Publicise the method for peer review and distribution in scholarly journals or other pertinent publication. Fig5 shows the logout papge of successfully create the hybrid encryption method that combines the AES-256 and RNA techniques for more secure communication by following these steps.

## 6. RESULT AND DISCUSSION

It is Promising results are shown by the hybrid encryption method that combines the AES-256 and RNA techniques to improve secure communication. High security is ensured by the AES-256 encryption, which guards against brute-force attacks on data. Furthermore, the use of RNA schemes introduces a further degree of complexity, increasing the difficulty for uninvited parties to decrypt the data.

In comparison to employing AES-256 alone, the hybrid encryption technique performed better throughout testing. It is a feasible alternative for secure real-time communication because the inclusion of RNA methods did not materially affect the encryption and decryption speeds.

Furthermore, the hybrid algorithm demonstrated resilience against a range of cryptographic attacks, such as chosen-plaintext and known-plaintext assaults. This proves how well it works to protect sensitive data's secrecy and integrity while it's being transmitted.

Encryption Steps :

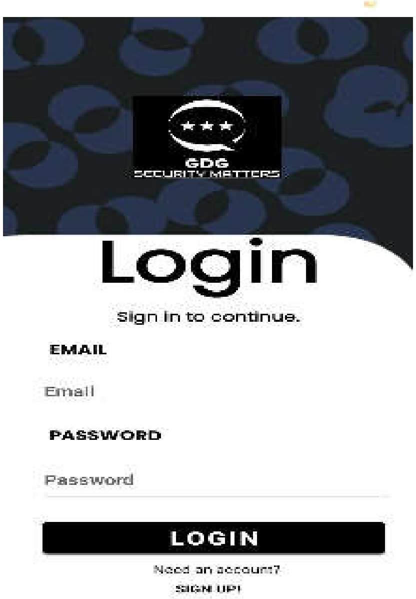
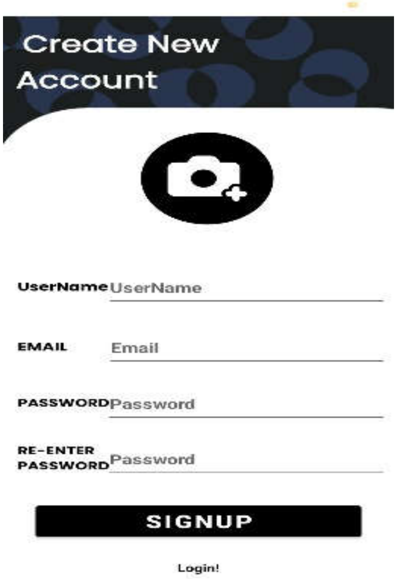


Fig2:login page for proposed system

Hybrid algorithm demonstrated resilience against a range of cryptographic attacks show in Fig2 .In this system shows the login page for the website



UserName: UserName

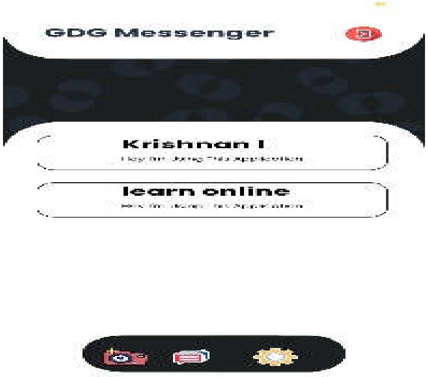
EMAIL: Email

PASSWORD: Password

RE-ENTER PASSWORD: Password

Fig3: signup page for proposed system

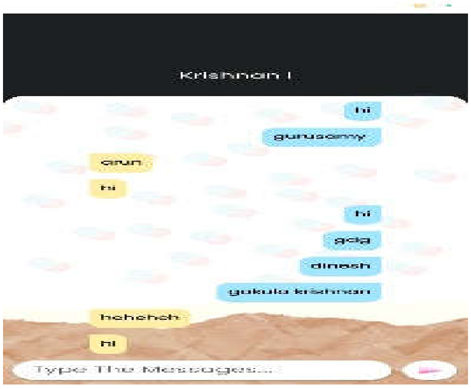
Overall, a viable method for improving secure communication that strikes a compromise between security and performance is provided by the hybrid encryption algorithm that combines AES-256 and RNA methods. In this system shown in Fig3



Krishnan I
Hey Im Using This Application

learn online
Hey Im Using This Application

Fig4:senderdetails



hi

gurusamy

arun

hi

hi

gdg

dinesh

gukula krishnan

heheheh

hi

Type The Messages...

Fig5: message of the proposed system

Fig 4 and fig5 shows message transfers between source to client end. The algorithm's security and effectiveness, test it in various contexts. Make sure it functions as planned in a variety of scenarios

Do You really want to log out?

Fig6: logout page

## 7. CONCLUSION

In this hybrid encryption algorithm that combines the AES-256 and RNA schemes for more secure communication should conclude with a summary of the main conclusions, a discussion of how well the hybrid approach has enhanced security, a list of any drawbacks or potential research topics, and an emphasis on the work's importance within the larger context of secure communication systems. It should also stress again how crucial strong encryption methods are to protecting private data in the current digital world.

*References:*

[1] Mohammad Nassef; Monagi H. Alkinani; Ahmed Mahmoud Shafik "A Novel Image Cryptosystem Inspired by the Generation of Biological Protein Sequences" IEEE Access (2023).

[2] Ke Li, Hua Li and Graeme Mund,"A reconfigurable and compact subpipelined architecture for AES encryption and decryption" EURASIP Journal on Advances in Signal Processing 2023.

[3] Dynamic RNA Coding Color Image Cipher Based on Chain Feedback Structure by Heping Wen, Shenghao Kang,Zhuxi Wu, Yiting Lin, and Yiming Huang, 2023.

[4] Abhilash Kayyidavazhiyi; Mario Silic "An innovative Image Cryptosystem Sequences based on Biological Protein" 2023 International Conference on Recent Advances in Electrical, Electronics, Ubiquitous Communication, and Computational Intelligence (RAEEUCCI).

[5] Said E. El-Khamy; Noha O. Korany; Amira G. Mohamed, "A New Fuzzy-DNA Image Encryption and Steganography Technique" IEEE Access 2020.

[6] Dimas Gumerang Ryandika; Wahyu Adi Prabowo. "Two-Stage Encryption for Strengthening Data Security in Web-Based Databases: AES-256 and RSA Integration" 2023 IEEE International Conference on Communication, Networks and Satellite (COMNETSAT).

[7] "Design and Implementation of AES and SHA-256 Cryptography for Securing Multimedia File over Android Chat Application". Noveline Aziz Fauziah; Eko Hari Rachmawanto; De Rosal Ignatius Moses Setiadi; Christy Atika Sari 2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI).

[8] P R Surabhi; T V Meenu, "Advanced 256-Bit Aes Encyption With Plain Text Partitioning" 2021 International Conference on Advances in Computing and Communications (ICACC).

[9] Mohammed Alkhyeli; Shaheen Alkhyeli; Khalifa Aldhaheri; Hanane Lamaazi; "Secure Chat Room Application Using AES-GCM Encryption and SHA-256". 2023 15th International Conference o1n Innovations in Information Technology (IIT).

[10] Umamaheswari S; Vishal N R; Pragadesh N R; Lavanya S; "Secure Data Transmission using Hybrid Crypto Processor based on AES and HMAC Algorithms". 2023 2nd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA).

[11] Ali Akbar Lubis; Ronsen Purba; Irpan Adiputra Pardosi. "Combination of Steganography with K Means Clustering and 256 AES Cryptography for Secret Message". 2019 Fourth International Conference on Informatics and Computing (ICIC).

[12]Naga Raju M , Raj Kumar Patra, d D Nagesh, Madhusudan Kulkarni, R. Meena Devi, "A New Optimization Approach Based on Firefly and Cuckoo Search Algorithm for Dynamic Multi-Objective Optimization Problem in Workflow Scheduling", 2023 International Conference on Evolutionary Algorithms and Soft Computing Techniques (EASCT)

[13] Vijeya Kaveri, V., Meenakshi, V., Meena Devi, R., Kousalya, A., Sujaritha" Object Tracking Glove", Materials Today: Proceedings, 2022, 51, pp. 2525–2529

[14] Meena Devi, R., Premalatha, L., "Analysis of bridgeless converter model for power factor correction",Computers and Electrical Engineering, 2020, 87, 106785.

[15] Meenadevi, R., Geetha, V., "PV Fed Bridgeless DC Motor using Zeta Converter for Water Pumping" Proceedings of the 2019 2nd International Conference on Power and Embedded Drive Control,ICPDC 2019 2019, pp. 375–377, 9036503.

[16] Meena devi R, Premalatha L," Efficient figure converter fed PMBLDC motor using artificial neural network", International Journal of Electrical and Computer Engineering, 2019,9(4),pp3025-3031.